REC'D 10 MAY 2006
WIPO PCT

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PCT-153	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP 03/14978	International filing date *(day/month/year)* 29.12.2003	Priority date *(day/month/year)* 29.12.2003
International Patent Classification (IPC) or both national classification and IPC INV. H04L29/06		
Applicant TELEFONAKTIEBOLAGET LM ERICSSON (publ) et al		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 9 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the opinion
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☒ Lack of unity of invention
   - V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand 05.07.2005	Date of completion of this report 09.05.2006
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Günther, S Telephone No. +49 89 2399-6962

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP 03/14978

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:

Description, Pages

1-29 as originally filed

Claims, Numbers

1-29 received on 30.09.2005 with letter of 29.09.2005

Drawings, Sheets

1/3-3/3 as originally filed

2. With regard to the **language,** all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).

   ☐ the language of publication of the international application (under Rule 48.3(b)).

   ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   ☐ contained in the international application in written form.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority in written form.

   ☐ furnished subsequently to this Authority in computer readable form.

   ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   ☐ the description, pages:

   ☐ the claims, Nos.:

   ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

IV. Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees, the applicant has:

   ☐ restricted the claims.

   ☐ paid additional fees.

   ☐ paid additional fees under protest.

   ☒ neither restricted nor paid additional fees.

2. ☐ This Authority found that the requirement of unity of invention is not complied with and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

   ☐ complied with.

   ☒ not complied with for the following reasons:

   see separate sheet

4. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this report:

   ☐ all parts.

   ☒ the parts relating to claims Nos. 1-3,17-20 .

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-3,17-20
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-3,17-20
Industrial applicability (IA)	Yes:	Claims	1-3,17-20
	No:	Claims	

2. Citations and explanations

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP 03/14978

see separate sheet

Re Item IV

Lack of unity of invention

1. This International Examining Authority found multiple inventions in this international application, as follows:

(I) Independent claims 1, 17, 21 (part) are directed to secure user authentication in a telecommunication core network. This is achieved by an authentication gateway, a user' equipment, means for and steps of carrying out an authentication procedure; computing a secret user's key; deriving, storing and confirming user's shared keys, sending the user's shared key along with the user's identifier.

(II) Independent claims 4 and 21 (part) are directed to management of master session records for registered users. This is achieved by a session manager, means for and steps of receiving user's shared keys and user's identifiers, creating a master session, checking whether user's shared key matches the shared key in user's master session.

(III) Independent claim 8 is directed to access control to services during active sessions. This is achieved by a service access authentication node, means for and steps of verifying whether an active session is indicated, assessing that user's shared keys are stored, determining a key match, granting access to the requested service.

2. Sending and receiving user's shared keys is common general knowledge, which is, e.g., known from the exchange of symmetric content encryption/decryption keys between content owner and content user in data networks.

3. Consequently, neither the objective problems underlying the subjects of the three claimed inventions, nor the solutions as defined by the special technical features described allow for the link of a common inventive concept to be established between said inventions. In conclusion, the three groups of claims are not linked by a single general inventive concept. The application hence does not meet the requirements of unity of invention as defined in Rules 13.1 and 13.2 PCT.

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. The following documents are referred to in this communication; the numbering will be adhered to in the rest of the procedure:

   D1: 3GPP TS 33.234 "Wireless Local Area Network (WLAN) Interworking Security", XP002282973

   D2: "SECURE AUTHENTICATION SYSTEM FOR PUBLIC WLAN ROAMING", XP001046692

2. Claim 1 does not fulfil the requirements of Article 33(1) PCT, because its subject-matter is not inventive, Article 33(3) PCT.

2.1. D1 discloses according to most of the features of apparatus claim 1 (the references in parentheses applying to D1):

an authentication gateway ("3GPP AAA server", page 11, line 21 and Fig. 4.3) arranged for receiving an access request in a telecommunication core network from an entity in an access network where a user with a user's equipment accesses through, the user being subscriber of the telecommunication core network and being identified by a user's identifier included in the access request, the authentication gateway having:

- means for carrying out an authentication procedure with the user's equipment through the access network in order to authenticate the user (page 11, lines 22-24),
- means for computing at least one secret user's key ("EAP-SIM derived key", page 23, lines 39) usable as cryptographic material,
- means for deriving from the cryptographic material a user's shared key (page 23, lines 34, 39-40).

2.2. The subject-matter of claim 1 differs from the disclosure in D1 in means for sending for SSO authentication purposes the user's shared key along with the user's identifier.

2.3. The objective technical problem is subsequent authentication of an authenticated user without further user interaction.

2.4. Means for sending for SSO authentication purposes the user's shared key along with the user's identifier is a common measure, which is, e.g., known from forwarding RADIUS authentication messages to the home provider when roaming across different providers, which is disclosed in D2, page 115, left-handed column, lines 10-13. Taking this meaure is supported by the hint in D1 to support trust between two different providers/operators based on a roaming agreement or Single-Sign-On solutions, see page 43, lines 24-28 and Fig. B.1)

It should be mentioned that the broad term "service network" may be interpreted to comprise any wireless access network, cellular operator's network or application layer service network like a WAP infrastructure.

3. Independent claim 17 does not fulfil the requirements of Article 33(1) PCT; because its subject-matter is not inventive, Article 33(3) PCT.

3.1. Most of the features of apparatus claim 17 correspond to the features of apparatus claim 1, and, in addition, claim 17 mentions a user's equipment, means for confirming the user's shared key and a repository for storing the keys, which is also known from D1 (Fig. 7.2.; page 24, lines 5-8; page 11, line 4).

4. The additional features of the dependent claims do not add anything inventive to the independent claims because the features are either known from the above cited prior art (processing key to obtain a key code MAC) or are common measures (notification about established or terminated session at access level, means for downloading a plug-in, receiving a SSO cookie).

CLAIMS

1. An Authentication Gateway (AG) arranged for receiving (S-23) an access request in a telecommunication core network (CN) from an entity (WLAN-AS) in an access network (WLAN) where a user with a user's equipment (UE) accesses through, the user being subscriber of the telecommunication core network (CN) and being identified by a user's identifier included in the access request, the Authentication Gateway having:

- means for carrying out (S-25) an authentication procedure (SIM-based; AKA; EAP) with the user's equipment (UE) through the access network (WLAN) in order to authenticate the user;

- means for computing at least one secret user's key (K_c) usable as cryptographic material; and

- means for deriving (S-251) from the cryptographic material (K_c) a user's shared key (SSO_key-1);

and **characterised by** comprising:

- means for sending (S-30) for SSO authentication purposes the user's shared key (SSO_key-1) along with the user's identifier towards a session manager (SSO_SM) serving a service network (SN).

2. The Authentication Gateway of claim 1, further comprising means for being notified (S-29) that a session at the access level has been established, this notification triggering the sending (S-30) of the user's shared key (SSO_key-1) towards the session manager (SSO_SM) serving the service network (SN).

3. The Authentication Gateway of claim 2, further comprising means for being notified that a session at the access

level has been terminated (accounting stop message), and means for forwarding this notification towards the session manager (SSO_SM) serving the service network (SN) in order to inactivate a current master session for the user.

4. A session manager (SSO_SM) serving a service network (SN) for SSO purposes and arranged for managing a session record for a user accessing the service network (SN) through an access network (WLAN), the user having been authenticated by a telecommunication core network (CN) where the user holds a subscription, the session manager (SSO_SM) **characterised in that** comprises:

- means for receiving (S-30) a first user's shared key (SSO_key-1) and a user's identifier from an Authentication Gateway (AG) of the core network (CN) for SSO authentication purposes, this first user's shared key (SSO_key-1) obtainable during the authentication of the user by the core network (CN);

- means for creating (S-301) a master session for the user that comprises the user's identifier and the received first user's shared key (SSO_key-1); and

- means for checking (S-34) whether a second user's shared key (SSO_key-2) derived at the user's equipment (UE) and received from a service access authentication node (SAAN) of the service network (SN) matches the first user's shared key (SSO_key-1) included in the master session for the user.

5. The session manager of claim 4, further including means for creating a service session to index the master session, in case of matching first and second user's shared keys, this service session intended as a token of a successful SSO user authentication.

6. The session manager of claim 5, further including means for verifying whether a service session indexes an active master session for a user to determine if a previous SSO authentication is still valid.

7. The session manager of claim 4, wherein the means for checking (S-34), whether a second user's shared key (SSO_key-2) derived at the user's equipment (UE) matches the first user's shared key (SSO_key-1) included in the master session, comprises means for processing the first user's shared key (SSO_key-1) to obtain a first key code (MAC(SSO_key-1)) to be matched against a second key code (MAC(SSO_key-2)) originated from the user's equipment.

8. A service access authentication node (SAAN) intended for receiving (S-31) a request from a user accessing a telecommunication service network (SN) through an access network (WLAN) with a user's equipment (UE), the user already authenticated by a telecommunication core network (CN) where the user holds a subscription, the request including a user's identifier to identify the user, the service access authentication node **characterised by** comprising:

- means for verifying whether an active service session is indicated in the request from the user's equipment;
- means for obtaining (S-33) a user's shared key (SSO_key-2) derived at the user's equipment (UE) and stored therein; and
- means for determining (S-34) in cooperation with a session manager (SSO_SM) serving the service network (SN) for SSO purposes whether the user's shared key (SSO_key-2) at the user's equipment (UE) matches the one stored in the master session (SSO_key-1) for the user.

9. The service access authentication node (SAAN)of claim 8, further comprising means for obtaining a service session for a user from the session manager (SSO_SM) serving the service network (SN) for SSO purposes.

10. The service access authentication node (SAAN)of claim 9, further including means for generating an SSO cookie to be submitted (S-37) to the user's equipment (UE), the SSO cookie comprising the service session.

11. The service access authentication node (SAAN)of claim 10, further comprising means for receiving an SSO cookie from the user's equipment (UE), the SSO cookie indicating a service session for the user.

12. The service access authentication node (SAAN)of claim 8, further comprising means for downloading an SSO plug-in towards the user's equipment, the SSO plug-in running for confirming back the user's shared key (SSO_key-2).

13. The service access authentication node (SAAN)of claim 8, wherein the means for obtaining (S-33) a user's shared key (SSO_key-2) derived at the user's equipment (UE) includes means for receiving from the user's equipment an element selected from:

- a key code (MAC(SSO_key-2)) obtainable by processing the user's shared key (SSO_key-2) at the user's equipment; and

- the user's shared key (SSO_key-2).

14. The service access authentication node (SAAN)of claim 13, further comprising means for submitting the received element to a cooperating session manager (SSO_SM) serving the service network (SN) for SSO purposes.

15. A use of the service access authentication node (SAAN)of claim 8 as an HTTP Proxy receiving service requests (S-

31) from users accessing a service network (SN) in a Walled-Garden SSO model.

16. A use of the service access authentication node (SAAN) of claim 8 as an authentication node of an Identity Provider where a credential request (S-31) is received from a user accessing a service of a Service Provider (SP) in a Federated SSO model.

17. A user's equipment (UE) usable by a user with a subscription in a telecommunication network, and arranged to access a telecommunication service network (SN) through an access network (WLAN), the user's equipment (UE) having:

- means for carrying out (S-25) an authentication procedure (SIM-based; AKA; EAP) to authenticate the user with a core network (CN), where the user holds the subscription, through the access network (WLAN);

- means for computing at least one secret user's key (K_c) usable as cryptographic material;

- means (S-252) for deriving from the cryptographic material (K_c) a user's shared key (SSO_key-2); and

- a repository for storing the user's shared key (SSO_key-2);

and **characterised by** comprising:

- means for confirming (S-32, S-33) for SSO authentication purposes the user's shared key (SSO_key-2) derived at the user's equipment towards an entity (SAAN, SSO_SM) in the service network (SN).

18. The user's equipment of claim 17, wherein the means for confirming (S-32, S-33) includes means for downloading an SSO plug-in from an entity (SAAN, SSO_SM) in the service

network (SN), the SSO plug-in running for confirming back the user's shared key.

19. The user's equipment of claim 17, wherein the means for confirming (S-32, S-33) includes means for processing the user's shared key (SSO_key-2) to obtain a key code (MAC(SSO_key-2)) to be transmitted to an entity (SAAN, SSO_SM) in the service network (SN).

20. The user's equipment of claim 17, further comprising means for receiving an SSO cookie from an entity (SAAN, SSO_SM) in the service network, the SSO cookie to be included in all further service requests from the user's equipment as an SSO token.

21. A method for supporting Single Sign-On services for a user with a user's equipment (UE) arranged for accessing a telecommunication core network (CN) and service network (SN) through an access network (WLAN), the user being identified as subscriber of the telecommunication core network (CN) when accessing the access network (WLAN), the method comprising the steps of:

- carrying out (S-25) an authentication procedure for the user between an entity (AG, HLR) of the core network (CN) and the user's equipment (UE);

- computing at the entity (HLR, AG) of the core network (CN) at least one secret user's key (K_c) usable as cryptographic material;

- computing at the user's equipment (UE) at least one secret user's key (K_c) usable as cryptographic material;

- deriving (S-251) a first user's key (SSO_key-1) from the cryptographic material at the entity (AG) of the core network (CN); and

- deriving (S-252) a second user's key (SSO_key-2) from the cryptographic material at the user's equipment (UE);

and **characterised by** including the steps of:

- creating (S-301) a master session for the user at an entity (SAAN, SSO_SM) in the service network, the master session comprising a user's identifier and the first user's key (SSO_key-1) usable for SSO authentication purposes;

- confirming (S-32, S-33) for SSO authentication purposes the second user's shared key (SSO_key-2) derived at the user's equipment towards the entity (SAAN, SSO_SM) in the service network (SN);

- verifying (S-34) whether the second user's shared key (SSO_key-2) matches the first user's shared key (SSO_key-1) for the user at the entity (SAAN, SSO_SM) in the service network (SN); and

- granting (S-35, S-36, S-37) access to the requested service in the service network (SN) on matching the first and second user's shared keys.

22. The method of claim 21, wherein the step of verifying (S-34) the matching of the first and second user's shared keys further includes a step of creating a service session to index the master session, this service session intended as a token of a successful SSO authentication.

23. The method of claim 22, further including a step of generating an SSO cookie to be submitted to the user's equipment, the SSO cookie comprising the service session.

24. The method of claim 23, further comprising a step of verifying whether an active service session is indicated in the request from the user's equipment.

25. The method of claim 21, wherein the step of confirming (S-32, S-33) for SSO authentication purposes the second user's shared key (SSO_key-2) derived at the user's equipment, includes a step of downloading an SSN plug-in from an entity (SAAN, SSO_SM) in the service network (SN), the SSO plug-in running for confirming back the user's shared key (SSO_key-2).

26. The method of claim 21, wherein the step of confirming (S-32, S-33) for SSO authentication purposes the second user's shared key (SSO_key-2) stored at the user's equipment, includes a step of processing the user's shared key (SSO_key-2) to obtain a key code (MAC(SSO_key-2)) to be transmitted to an entity (SAAN, SSO_SM) in the service network (SN).

27. The method of claim 26, wherein the step of verifying (S-34) whether the second user's shared key (SSO_key-2) matches the first user's shared key (SSO_key-1) includes a step of processing at an entity (SAAN, SSO_SM) of the service network (SN) the first user's shared key (SSO_key-1) to obtain a first key code (MAC(SSO_key-1)) to be matched against a second key code (MAC(SSO_key-2)) originated from the user's equipment.

28. The method of claim 21, wherein the step of creating (S-301) a master session for the user at the entity (SAAN, SSO_SM) in the service network includes a step of receiving the first user's key (SSO_key-1) usable for SSO authentication purposes from an entity (AG) of the core network (CN).

29. The method of claim 21, wherein the step of creating (S-301) a master session for the user at the entity (SAAN,

SSO_SM) in the service network includes a step of initiating an access session (S-29) when the user accesses the access network.

5